UNITED STATES PATENT APPLICATION

PRINTER SECURITY KEY MANAGEMENT

INVENTORS

Curtis Reese
6204 Northview St.
Boise, ID 83704

Mark Josephsen
12508 W. Freedom Drive
Boise, ID 83713

Shane Konsella
4816 N. High Country Way
Star, ID 83669

Client Ref. No. 100202485-1

Printer Security Key Management

Field of the Invention

The invention relates generally to secure printing, and more specifically to a printer having encryption key management capability.

Background of the Invention

Printers typically print a document received from an attached computer upon receipt of the digital information representing the document to be printed. Multiple users may be electronically attached to the same printer via a network, so that a single printer is used by several people. In some environments, printers can receive data to be printed by other means also, including via a wireless or infrared network rather than via a wired network.

When several users or computer systems share access to a single printer, the printed documents are usually printed in the order they are sent to the printer, and left to be retrieved by the person printing each specific document. This system works adequately for environments in which the content of the printed documents is not secret or confidential, but works less well where the person printing a document may not want others who have physical access to the printer or use the same network to access the printed data.

One solution is to set up a mailbox on a shared printer that receives a matter, but does not print it until the user owning the mailbox enters a pin number or other identifier indicating that they are present at the printer. This enables the person printing the document to retrieve the pages as they are printed, even when the printer is not located near the computer that was used to print the document.

Although this solution prevents those sharing a printer from intercepting and reading documents printed by other users, it may not prevent those sharing the same network from intercepting or monitoring the network for print data and reading the data. Although this is beyond the ability of the average office worker, it is a real threat in environments such as banking, human resources, government, and other such businesses that deal with particularly sensitive or confidential information.

There exists a need for methods and systems that address the security of such sensitive or confidential data.

Summary of the Invention

In one example embodiment of the invention, a printer module receives a message from an attached computer that is requesting a secure printing key. The printer module generates a key in response to the received message, and sends the key to the attached computer requesting the key. The printer module executes in some further embodiments of the invention in a Java virtual machine, and provides communication with the attached computers via a web server module executing within the printer.

Brief Description of the Figures

Fig. 1 shows a printer and attached computer system consistent with one embodiment of the present invention.

Fig. 2 is a flowchart illustrating a method of practicing one embodiment of the present invention.

Detailed Description

In the following detailed description of sample embodiments of the invention, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific sample embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical, electrical, and other changes may be made without departing from the scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the invention is defined only by the appended claims.

The present invention provides a printer module that in some embodiments is operable to receive a message from an attached computer that is requesting a secure printing key. The printer module generates a key in response to the received message, and sends the key to the attached computer requesting the key. The printer module executes in some further embodiments of the invention in a Java virtual machine, and provides communication with the attached computers via a web server module executing within the printer.

Figure 1 shows an example system upon which some embodiments of the present invention may be practiced. A printer device 101 prints received data on paper or other media for physically recording the data. The typical laser printer illustrated here, for example, processes paper from paper tray 102 and deposits toner from toner cartridge 103 on the paper to create a physical record of the data to be printed. Various other printers include inkjet, dye sublimation, and ribbon impact marking technology, and print on various media such as transparencies, envelopes, and photographic paper.

The printer 101 is here connected via connection 104 to a computerized system 105. The connection 104 in various embodiments of the invention comprises any of various types of connection operable to provide communication between the computer and printer, including parallel (IEEE 1284), Universal Serial Bus (USB), firewire (IEEE 1384), ethernet, and other such connections. The computerized system is further attached to a network such as network 106, and is employed by a user, who wishes access to the printer 101 for printing data.

In operation, the user of the computerized system 105 requests to send a document to the printer 101 using secure printing features of the printer. More specifically, the user first requests that the printer 101 generate encryption or security keys for use in encrypting data sent from the computerized system to the printer. A module within the printer receives the message requesting the secure printing key, generates the key, and sends the key to the user's computerized system 105 via connection 104. The computerized system 105 then stores the key, and uses it to encrypt data sent to printer 101 so that even if the document is intercepted over connection 104 the document cannot be easily interpreted or understood.

In some embodiments of the invention, the user requests the security key by accessing a web page hosted by a web server within the printer 101. In a further embodiment, the printer 101 executes the security module operable to generate and send keys in a Java virtual machine executing within the printer 101.

Generation of the security keys within the security module will take different forms in various embodiments of the invention. In one embodiment, a symmetric key is generated, and the symmetric key is transmitted to the attached computer requesting the key via connection 104 only after a secure connection has been negotiated between printer 101 and computer 105. This ensures the confidentiality of the symmetric key, which can be used to encrypt data or to decrypt data that has already been encrypted with the same symmetric key. A wide variety of algorithms using symmetric keys or block ciphers, including DES (Data Encryption Standard), IDEA, CAST, Twofish, Blowfish, MD5, and RC5, may be employed in this manner in various embodiments to ensure the confidentiality of data between the computerized system 105 and the printer 101.

In other embodiments of the invention, asymmetric algorithms may be employed, such as the public key/private key RSA system. In the public key/private key systems, the printer security module generates both a public and a private key. It retains the private key, and sends the public key to the computerized system 105. The public key can be used to encrypt data sent to the printer, but cannot be used to decrypt the encrypted data. This means that if the public key is sent to the requesting user of the computerized system 105 over an insecure link, the person intercepting the public key cannot decrypt data cannot use the key to decrypt data sent from the computerized system 105 to the printer 101, but can only encrypt data sent to the printer 101 as though he were the authorized user of the public key.

When the printer receives the data encrypted by the public key, it decrypts it using the private key, and either prints the data or stores the data until the user indicates he is ready for the data to be printed. Storing the data until the user confirms it is to be printed is useful in applications where a single printer is shared among many users or is located in a relatively public place. The user can then identify himself to the printer such as by entering a pin number, and cause the document to print when he is at the printer and able to ensure the physical security of the printed data.

Interception of data sent to the printer 101 from the computerized system 105 is a particularly significant risk when the connection 104 is a network connection, such as an ethernet network or an internet connection. In applications such as human resources management, banking, or national defense, it is often important that the printed data not be intercepted or viewed by unauthorized people, and that it not be altered. Encryption prevents viewing or altering data, and so is employed to ensure the security of the transmitted data.

(Figure 2 is a flowchart illustrating a method of managing security keys within a printer, consistent with an embodiment of the present invention.) Duplicate?

Figure 2 is a flowchart, showing a method of practicing one embodiment of the present invention. A user wishing to use a printer connected to a network first identifies the printer and requests a key from the printer at 201. The key is requested in some embodiments via a web browser interface, via the printer driver, or via other methods. The printer receives the key request at 202, and sends the request to the security module within the printer to produce a key at 203. The generated key in various embodiments of the invention may be a symmetric key, may be a public key that is a part of a public key/private key pair of generated keys, or may be another type of encryption or security key.

The generated key is then sent to the user's computerized system at 204, over what is desirably a secure connection between the printer and the computerized system in embodiments using symmetric encryption keys. The user can then use the received key to encrypt data to be printed at 205, so that when the data is sent to the printer at 206 it is sent in encrypted form that cannot be easily viewed or altered if it is intercepted.

When the printer receives the encrypted data, it uses its security key to decrypt the data at 207, and is then able to print the decrypted data at 208. In some further embodiments of the invention, the printer prints the data only after the user indicates physical presence at the printer, such as by entering a pin number or password, to further protect the physical security of the printed document.

The system presented here does not require a central key management authority, even for embodiments that use a public key/private key encryption algorithm, because the printer acts as its own trusted key management authority. Incorporation of key production and management functions into a security module within the printer provides a simpler system of key management, and a web browser-based interface to the security module provides users with a user-friendly interface to perform key management functions. Further embodiments of the invention will provide a variety of key management functions, including the ability to create, assign, delete, group, or otherwise manage the keys and users as is deemed appropriate for a particular application.

Although specific embodiments of a printer security key distribution system have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the invention. It is intended that this invention be limited only by the claims, and the full scope of equivalents thereof.